AMENDMENTS TO THE SPECIFICATION

Please replace paragraph [0033] with the following marked-up version of the paragraph:

[0033] As already described, the authentication module 116 can receive the authentication information 215 from a local contact database (e.g., 120, Figure 1) stored at a network provider 110, or can receive the information from an external or third party database 210 (e.g., from remote database 160, Figure 1). This can also be true for configuration information [[215]] 220. For example, in an organization, one server providing network service and device access can be separate from a server that provides contact and permissions information. An administrator can use a management application 205 (locally on the network provider, or remotely over a network) to manage how the centralized service 200 implements the authentication 215 and configuration information 220. Alternatively, the administrator can use the management application 205 to change identity and grouping information within each module (215, 220, etc.).

Please replace paragraph [0049] with the following marked-up version of the paragraph:

[0049] The inventive method further comprises a functional step 450 of exposing a network device to the client (e.g., client 100). Step 450 includes exposing the at least one device to the client through a specific one of a network port, a WWN, and a portal, such that the client can access the at least one device identified by the target when the client has access to the specific one of a network port, a WWN, and portal,[[,]] and when the client presents the associated client authorization to the network provider. Functional step 450 can be accomplished by performing the specific act 430 of assigning the target to a port via the protocol-independent port driver. Act 430 assigning the target to a port through a protocol-independent port driver at the network provider[[ ]]. For example, the centralized service 200 can assign target 380 to be client-accessible through a port (such as an iSCSI portal or a Fibre Channel WWN). Thus, if the port is dedicated to a specific workgroup or application, only those clients authorized on the specific workgroup or application can access targets 380 through the port as managed through one or more of the respective miniports 230, 235, etc.